



МУ МВД России «Иркутское»

ВИДЫ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ И ЗАЩИТА ОТ НИХ



**ОСТОРОЖНО,
МОШЕННИКИ!**



**МОШЕННИК
ЗВОНИТ ЖЕРТВЕ,
ПРОСИТ СООБЩИТЬ
СМС КОД, ПОД
ПРЕДЛОГОМ**



Сотрудника здравоохранения:

- Предлагает продлить срок действия страхового полиса;
- Запись по электронной очереди.

Сотрудника коммунальных служб:

- Предлагает замену электросчетчиков;
- Скачать приложение.

Сотрудника Госуслуг

- Сообщает о взломе личного кабинета.

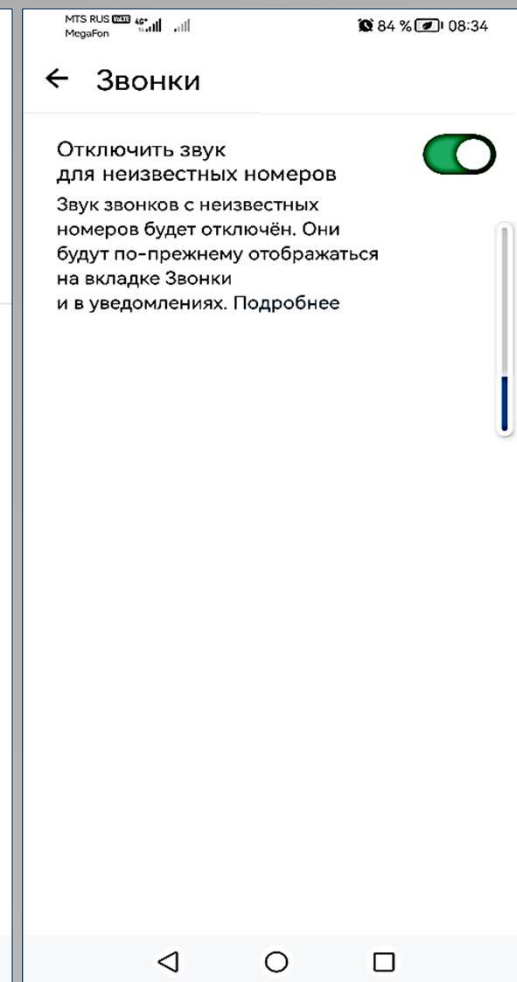
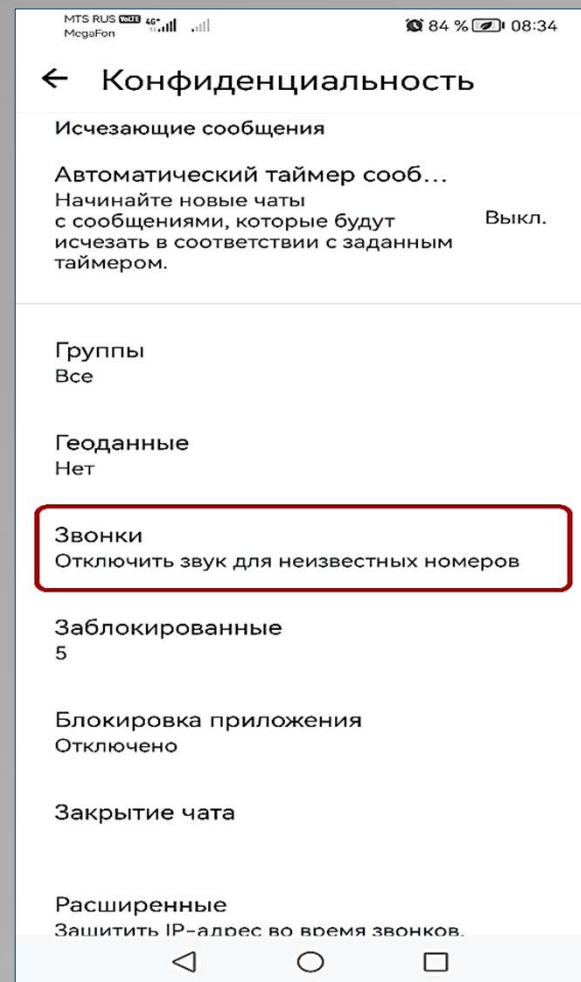
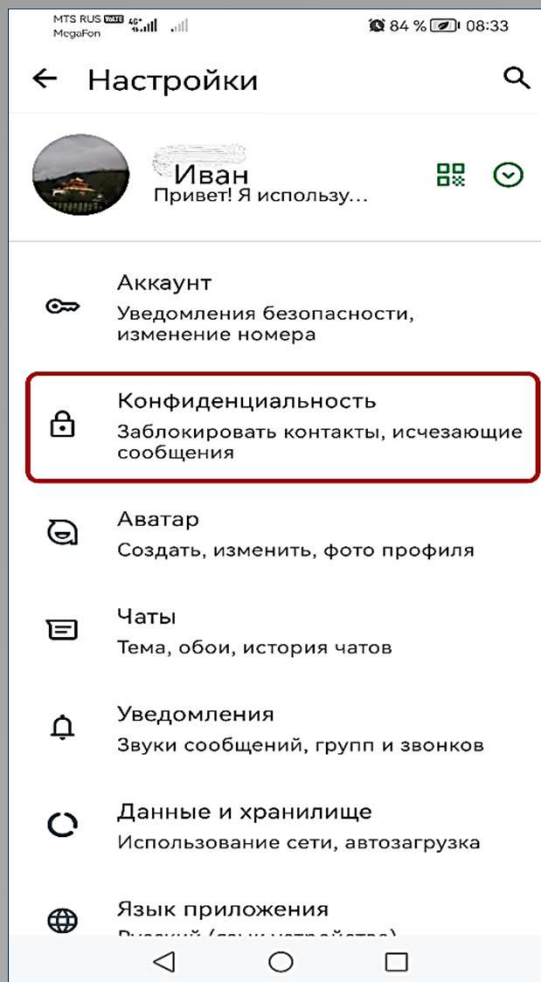
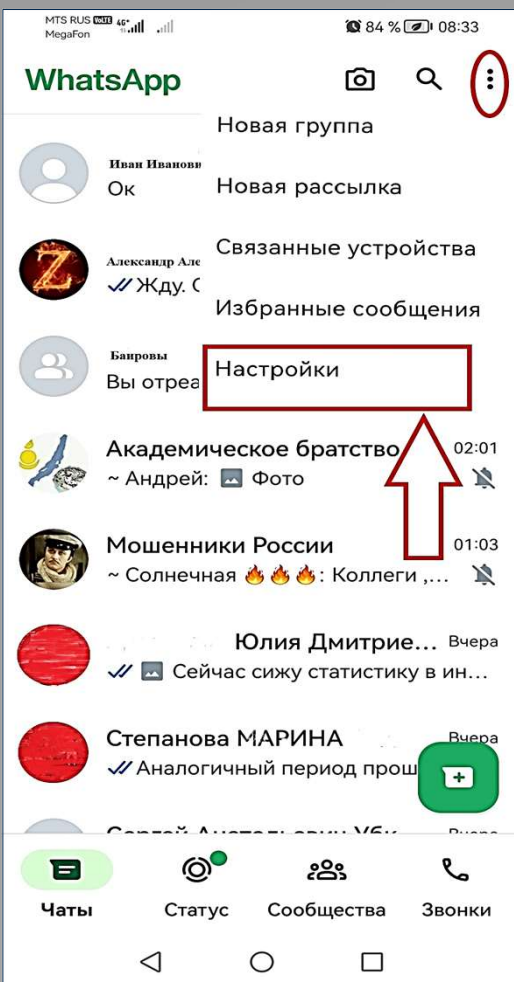


**Общий ущерб составляет
Более 2,5 млрд. рублей
(за 2024 год)**



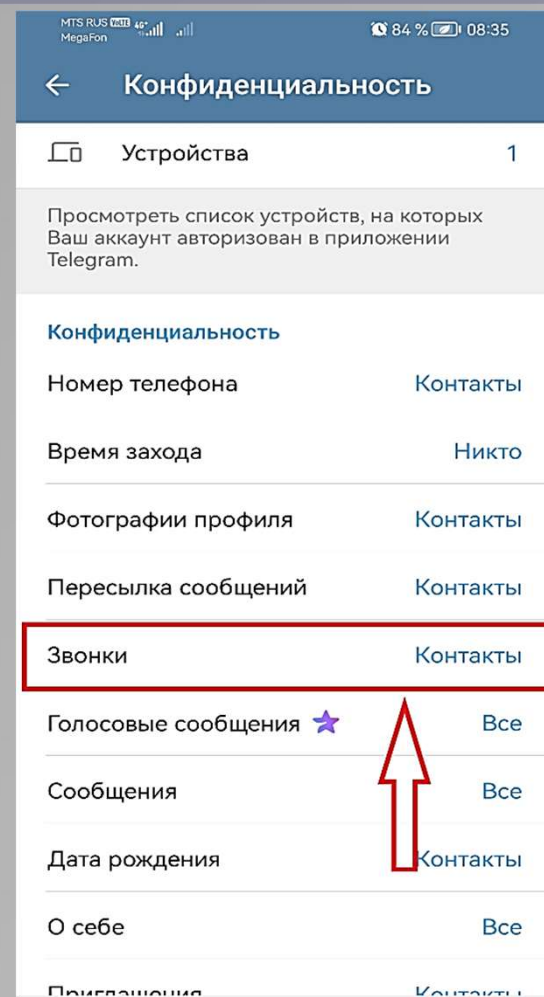
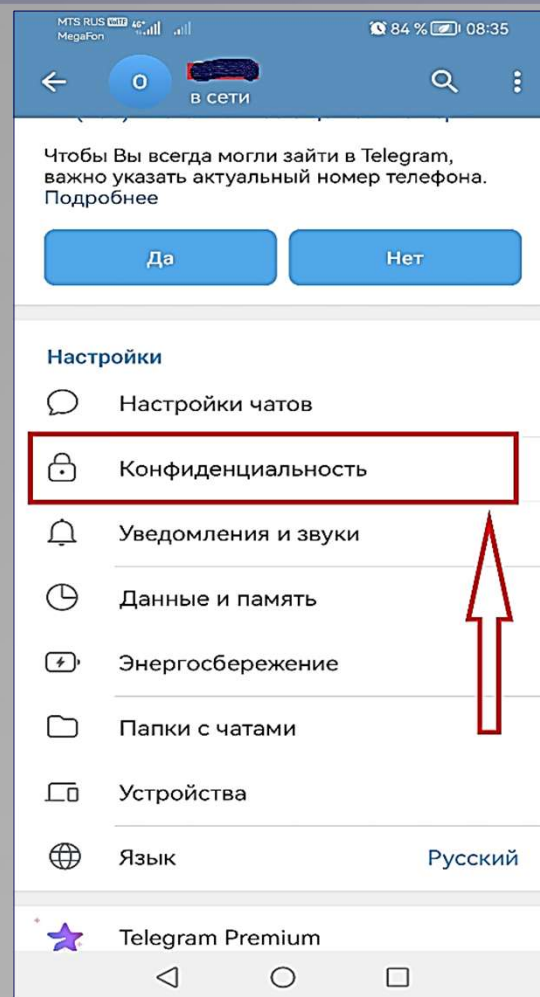
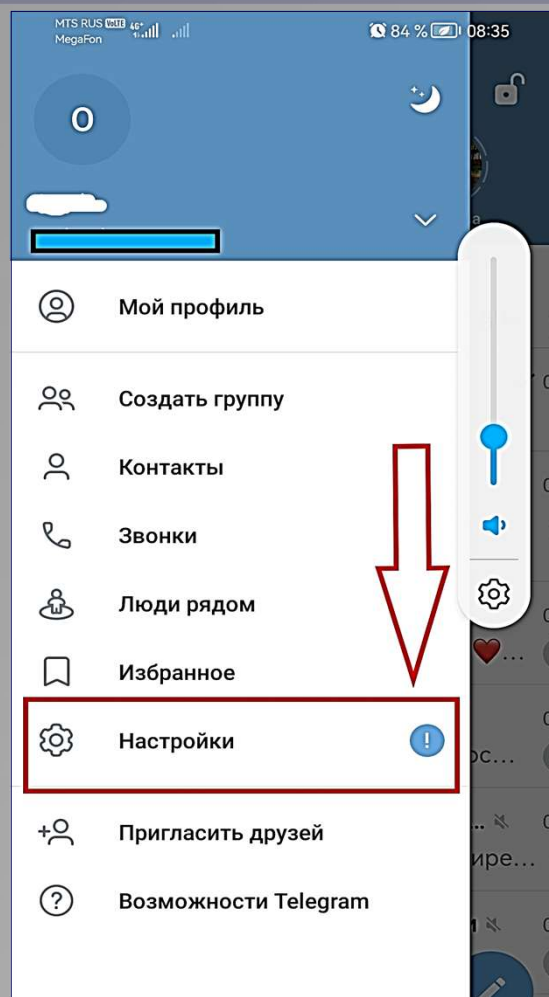
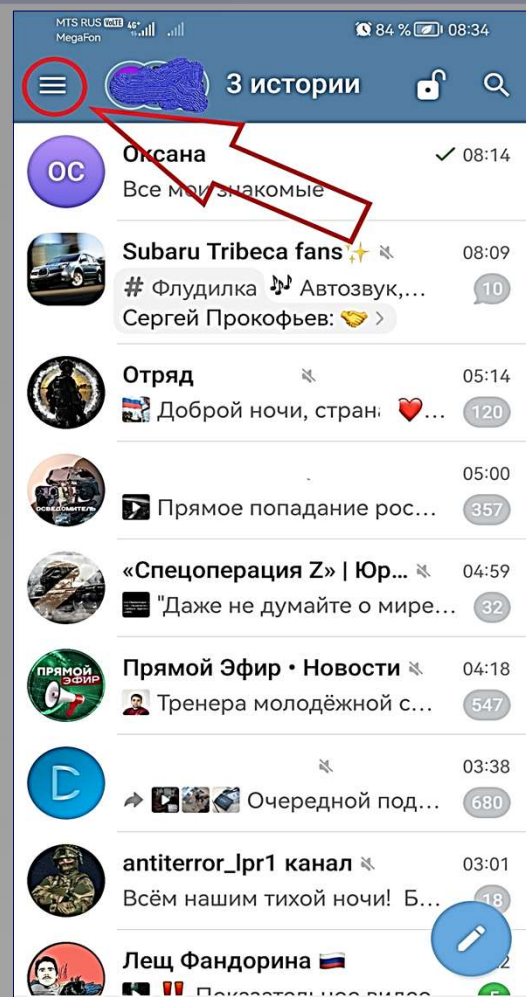


Защита от звонков в *WhatsApp*



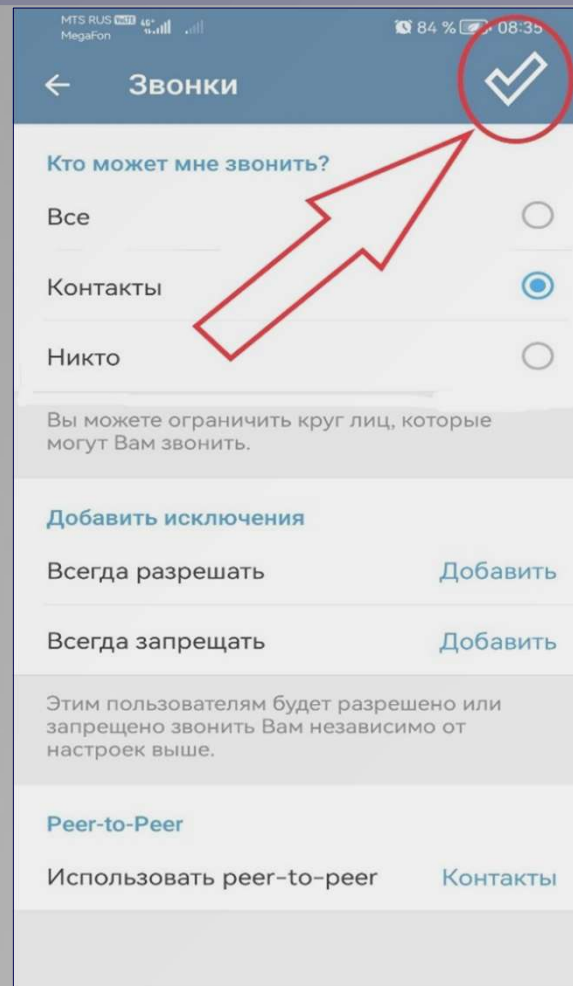
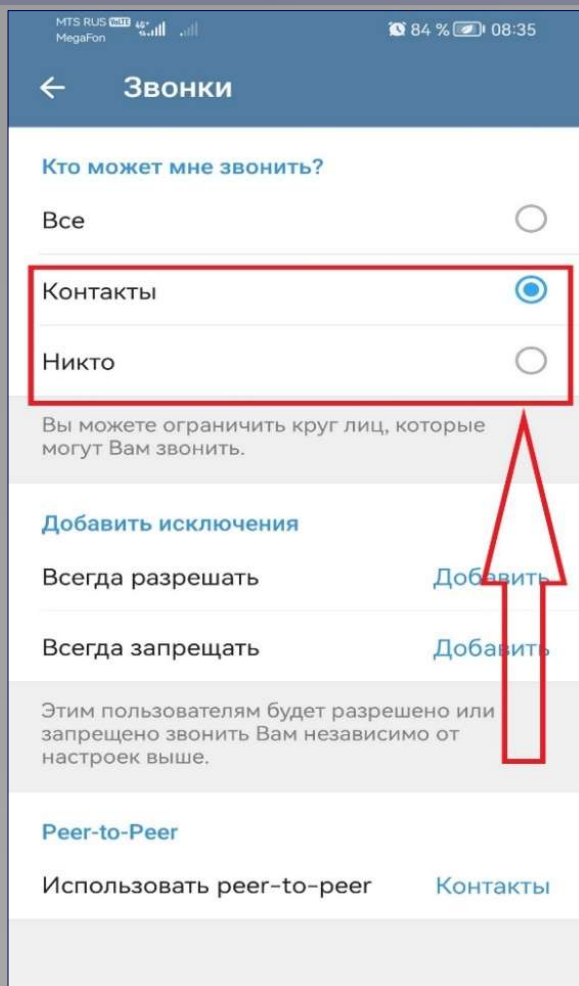


Защита от звонков в *Telegram*



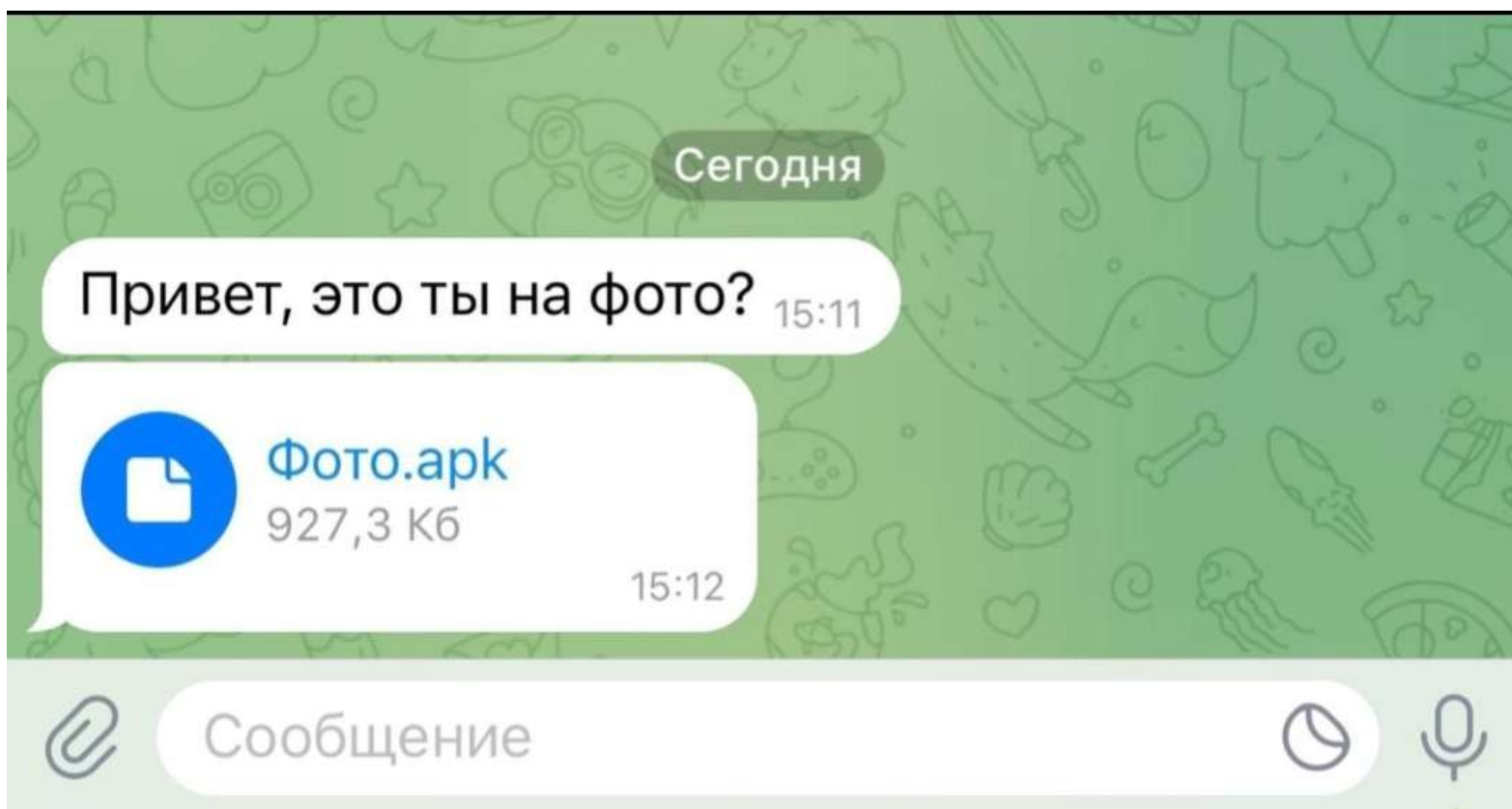


Защита от звонков в *Telegram*





Новый вид мошенничества в мессенджерах





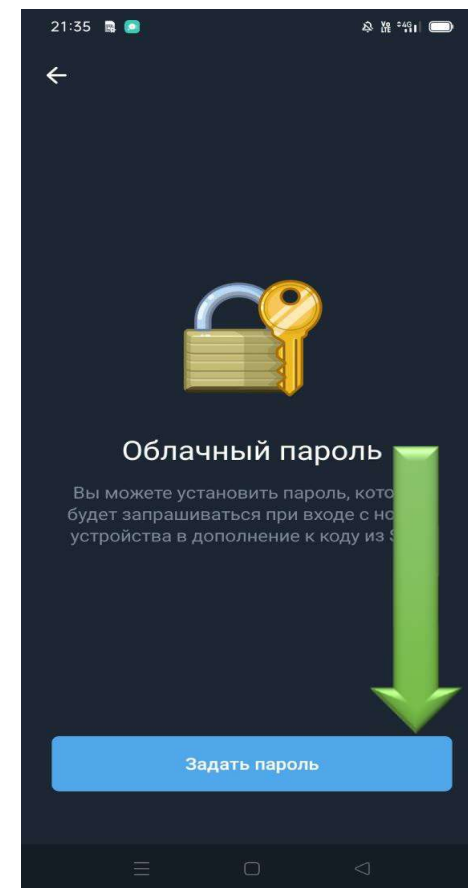
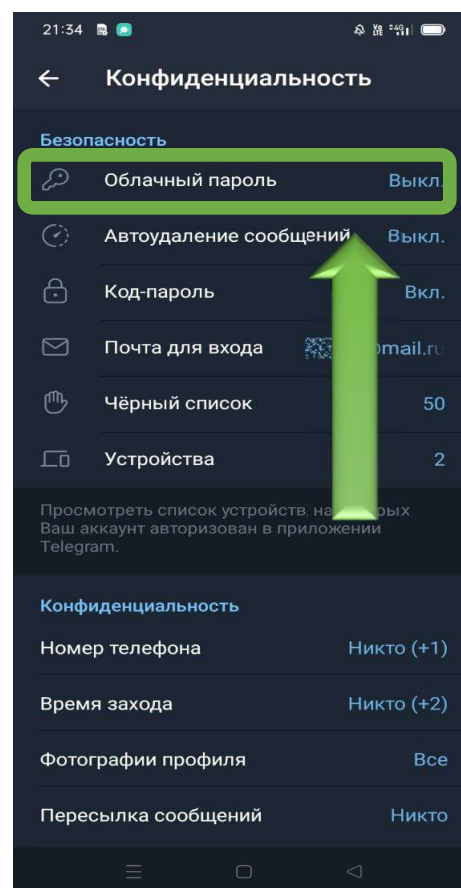
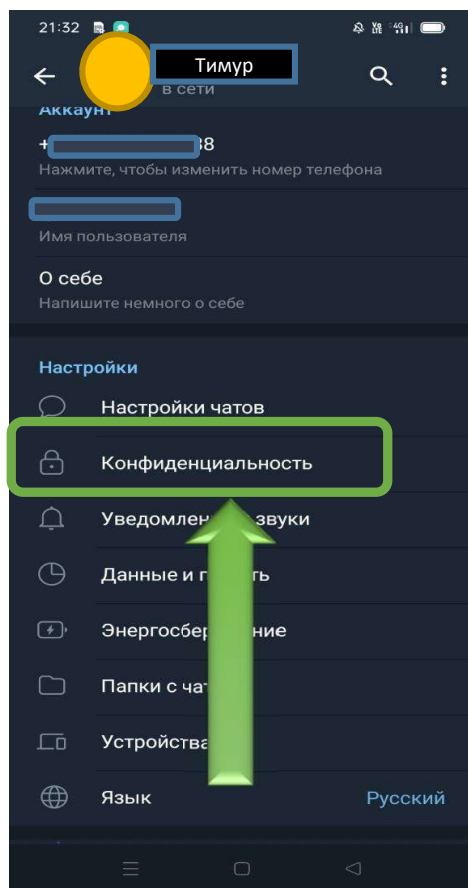
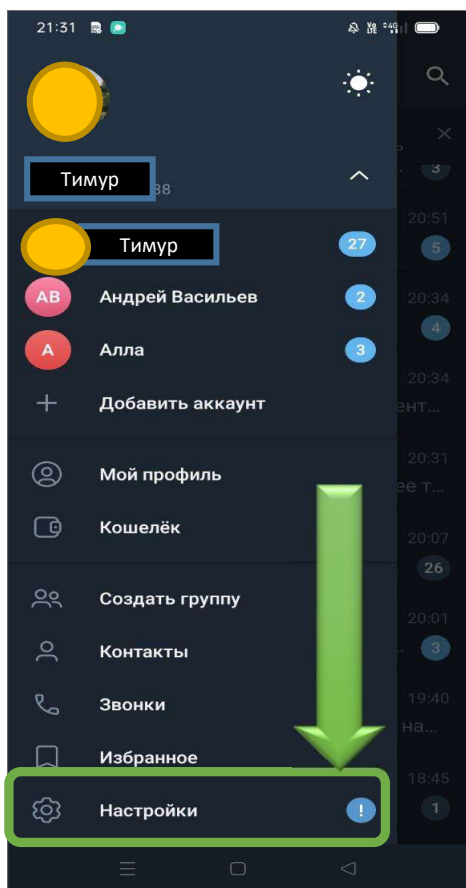
МУ МВД России «Иркутское»

Как настроить двухфакторную аутентификацию (проверку) в мессенджерах





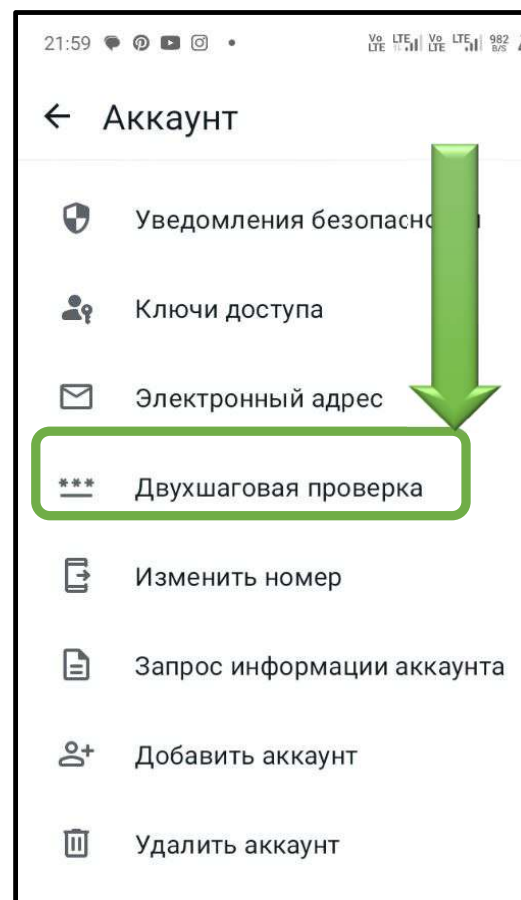
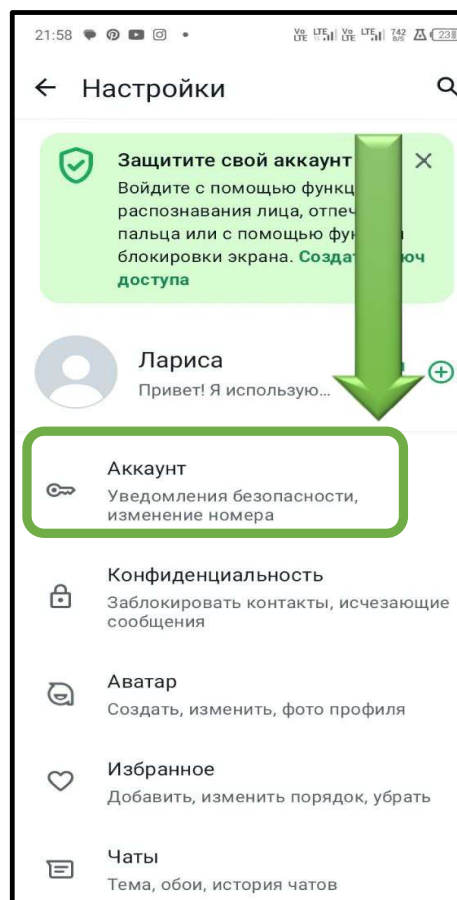
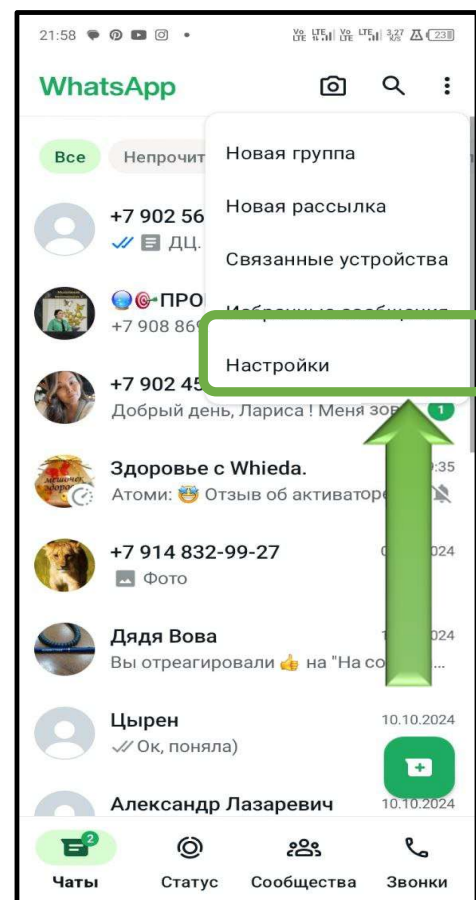
Как настроить двухфакторную аутентификацию в *Telegram*:



МУ МВД России «Иркутское»



Как настроить двухфакторную аутентификацию в *WhatsApp*:



МУ МВД России «Иркутское»



Советы по безопасности



Покупайте и продавайте в вашем городе, из рук в руки



Называйте только номер карты - этого достаточно для перевода денег



Оформите отдельную карту для оплаты в интернете



Не отправляйте деньги наперед



Настаивайте на наложенном платеже без предоплаты



Проверяйте данные продавца/покупателя в интернете



Как распознать сайт двойник?

► ПРИ ПРОВЕРКЕ ОБРАТИТЕ ВНИМАНИЕ НА ДОМЕН (ИМЯ) САЙТА:

- Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I» (onL1ne вместо onLine);
- Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);
- В некоторых случаях для написания домена используются буквы похожие на латинские из алфавита другого языка;
- Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU



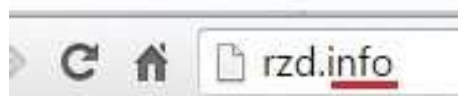
*мошенники в
Альфа.Клик*



*правильный сайт
Альфа.Клик*



*лишняя буква "t" сайт
ВКонтакте*



должно быть rzd.ru сайт РЖД



Проверьте продавца / покупателя при помощи различных сервисов. Например на сайте «Доверие в сети»

[Регистрация](#)[Статьи](#)[Топ 100 сайтов](#)[Логин](#)

ПРОВЕРКА НА МОШЕННИЧЕСТВО

[Сайты](#)[Соцсети](#)[Телефоны](#)



Признаки финансовой пирамиды

- 1** Обещание слишком высоких доходов
- 2** Прибыль за счет привлечения новых вкладчиков
- 3** Ограниченный доступ к учредительным документам и финансовой отчетности компании
- 4** Сомнительные договоры
- 5** Агрессивная реклама



Как себя обезопасить?

- Проверять брокерскую компанию на сайте Банка России на наличие лицензии (<https://cbr.ru/finorg/>);
- Не доверять рекламе о биржах в социальных сетях;
- Не верить заманчивым и убедительным обещаниям о высокой доходности и отсутствии риска.



МУ МВД России «Иркутское»

Как уберечь ребенка от преступных посягательств в цифровой среде



Как уберечь ребенка от преступных посягательств в цифровой среде

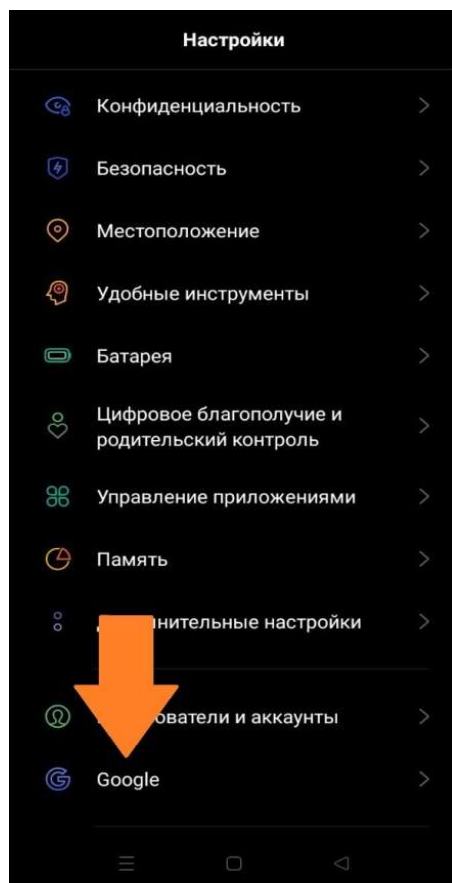
**Уделяйте больше внимания своему ребенку
Чаще разговаривайте с ним, чтобы он
делился с Вами о своем окружении, как
прошел его день и внимательно следите за
изменением в его поведении**



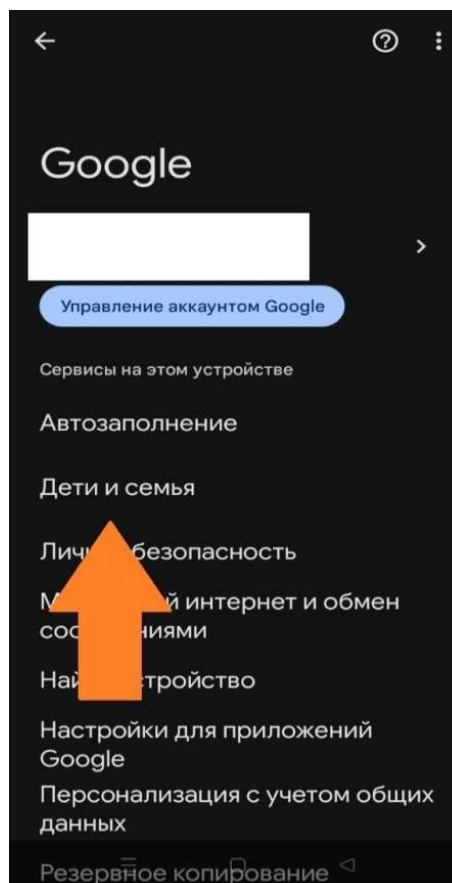
Установите дома родительский контроль на телевизор и его аккаунты в интернете.

1. Откройте «Настройки» на устройстве ребенка.

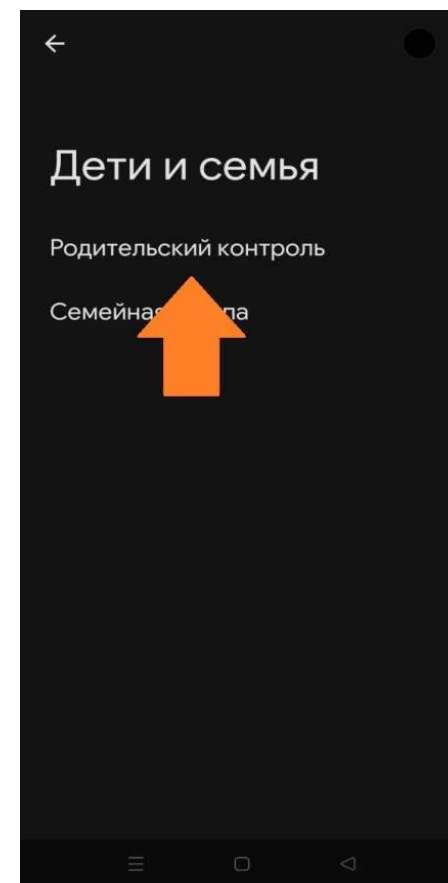
2. Выберите «Google»



3. «Дети и семья»



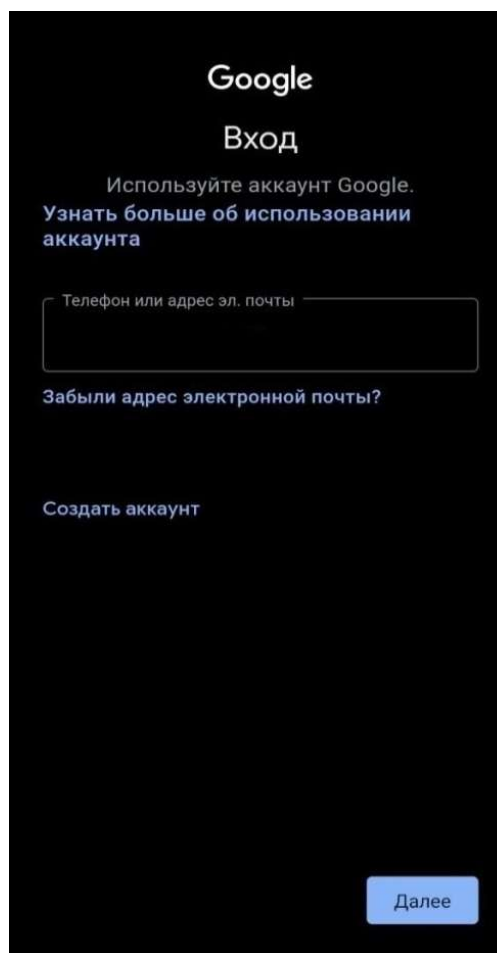
4. «Родительский контроль»



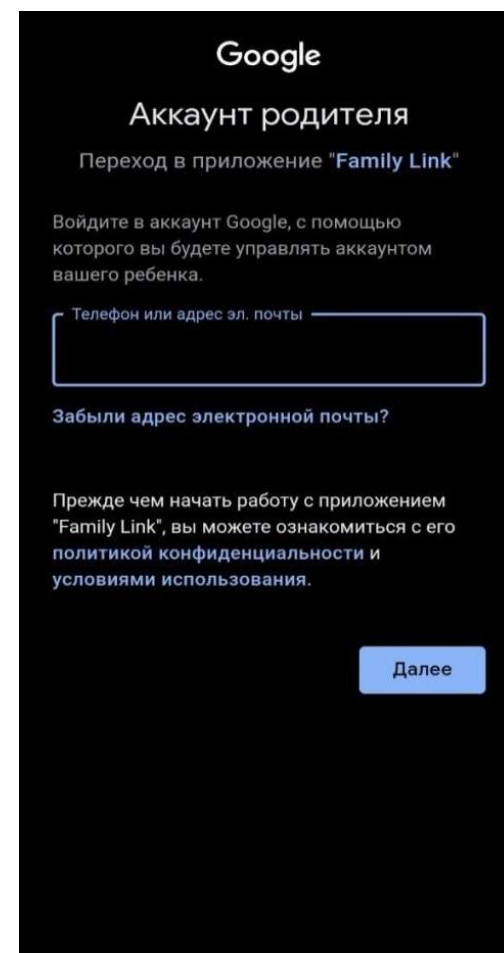
Нажмите «Приступить»



Выберите аккаунт ребенка или создайте новый.



Войдите в свой «родительский»





Будьте бдительны!!!



- ◇ **Контролируйте ребенка в социальных сетях, просматривайте кого он добавляет в друзья и с кем общается.**
- ◇ **Внимательно следите за финансовыми тратами своего ребенка.**
- ◇ **Если у него имеется банковская карта, кому и зачем он переводит денежные средства и какие осуществляет покупки.**
- ◇ **Объясните ребенку про цифровую гигиену.**



МУ МВД России «Иркутское»

Схемы взлома и защита от них





1. Звонок от работника сотового оператора

1. Поступает телефонный звонок от оператора сотовой связи, сообщают что необходимо продлить срок действия SIM-карты или обновить паспортные данные.
 - В это время мошенники, зная абонентский номер жертвы, на сайте «Госуслуги» открывают вкладку: «Восстановление пароля».
 - Указывают номер жертвы и ждут когда им сообщат код из SMS.
2. После чего, в целях подтверждения личности или под другим предлогом просят сообщить / продиктовать SMS-код, поступивший на телефон с портала «Госуслуги»
 - Для личных кабинетов, где установлен вход на портал по SMS-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. **На самом деле повторно приходит КОД для изменения номера телефона.**

госуслуги

Восстановление пароля

Телефон / Email
89000000000

госуслуги

Изменение номера телефона
+7 924

Новый номер телефона

+7 () - - -

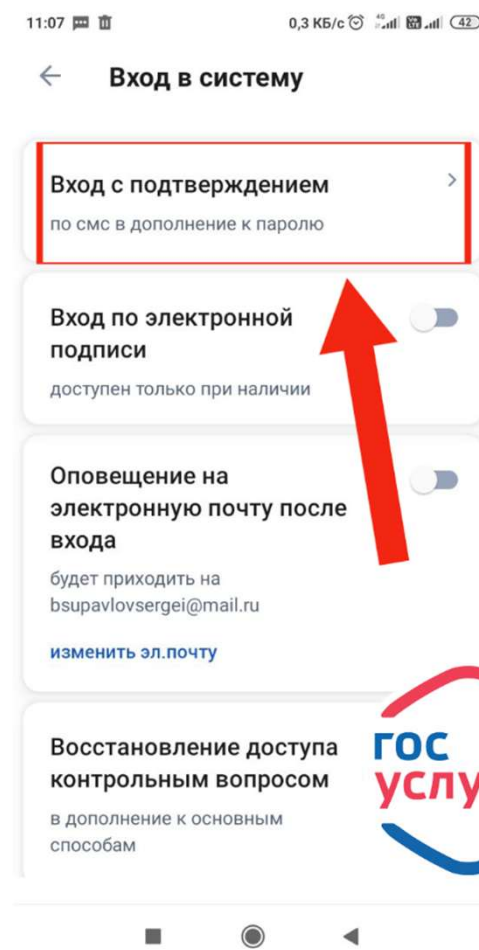
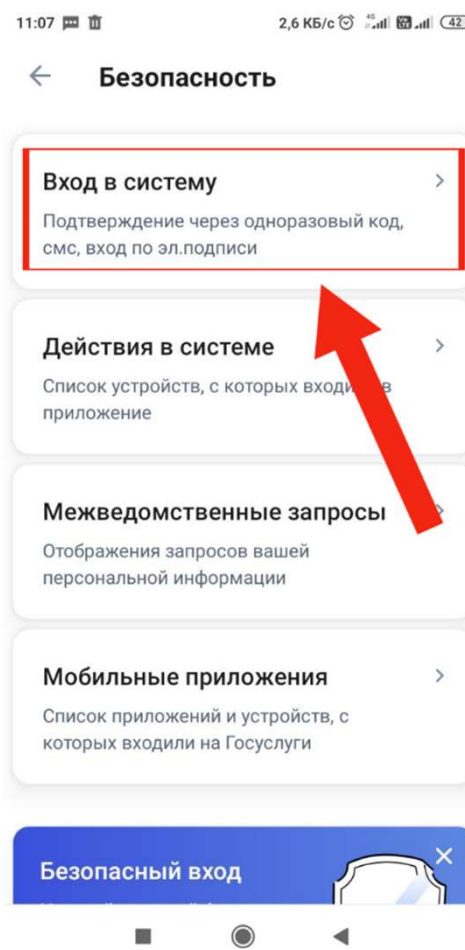
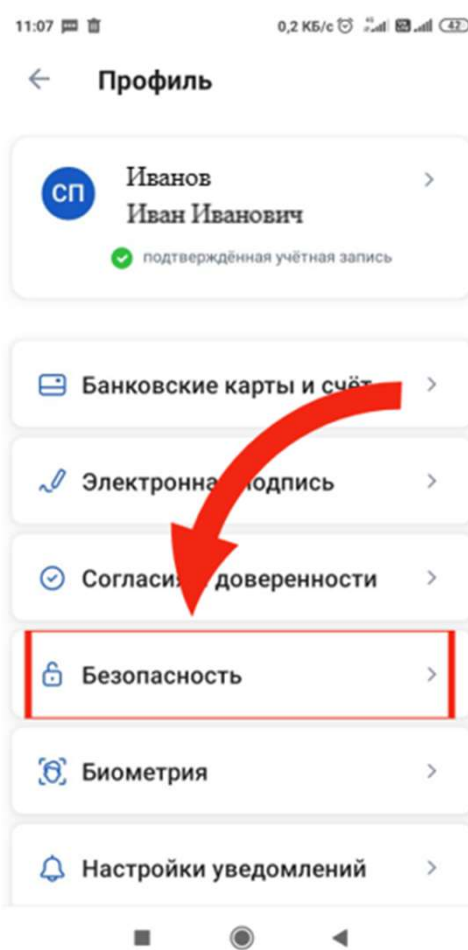
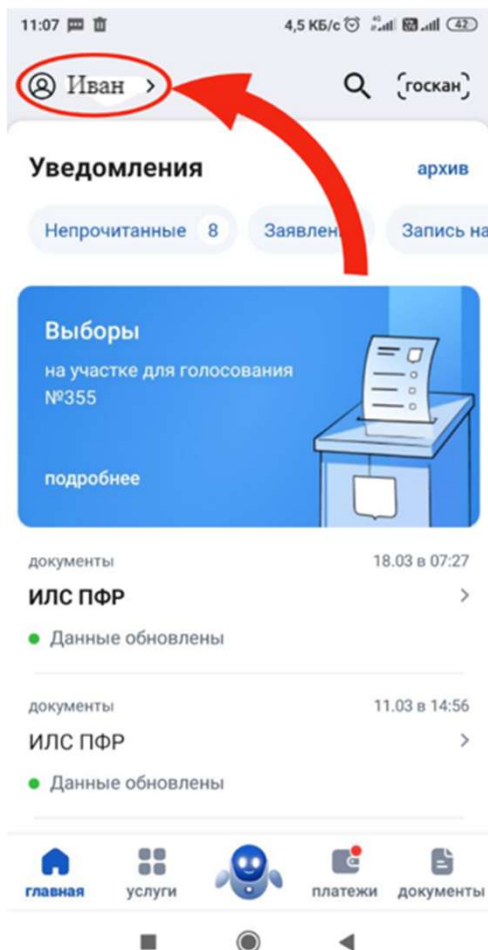


Как обезопасить личный кабинет от взлома?

1. Никому не сообщайте код из SMS-сообщения, поступившего с портала «Госуслуги»;
2. Настроить двухэтапную аутентификацию;
3. Отозвать неизвестные для вас согласия в личном кабинете;
4. Регулярно, раз в полгода необходимо менять пароли доступа.

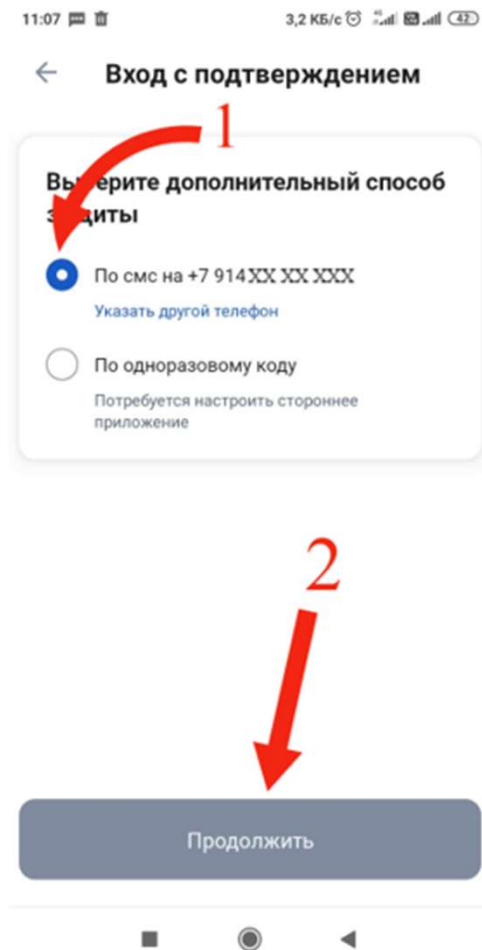


Дополнительная защита личного кабинета





Дополнительная защита личного кабинета



Функция входа с двухэтапной аутентификацией.

Войти в личный кабинет с помощью одного только логина и пароля будет недостаточно, при каждом входе в личный кабинет необходимо вводить одноразовый код, поступающий в виде SMS-сообщения.





Дополнительная защита личного кабинета

14:24 8,6 КБ/с 14:24 4,7 КБ/с

← **Вход в систему**

Вход с подтверждением >
по sms в дополнение к паролю

Вход по электронной подписи ☐
доступен только при наличии

Оповещение на электронную почту после входа ☐
будет приходить на
bsupavlovsergei@mail.ru
[изменить эл.почту](#)

Восстановление доступа контрольным вопросом ☒
в дополнение к основным способам

Ваш контрольный вопрос
Выберите вопрос 1

Ответ на контрольный вопрос
Введите ответ 2

Введите пароль, чтобы подтвердить использование контрольного вопроса для восстановления доступа
Введите пароль 3

Изменить 4 Включить

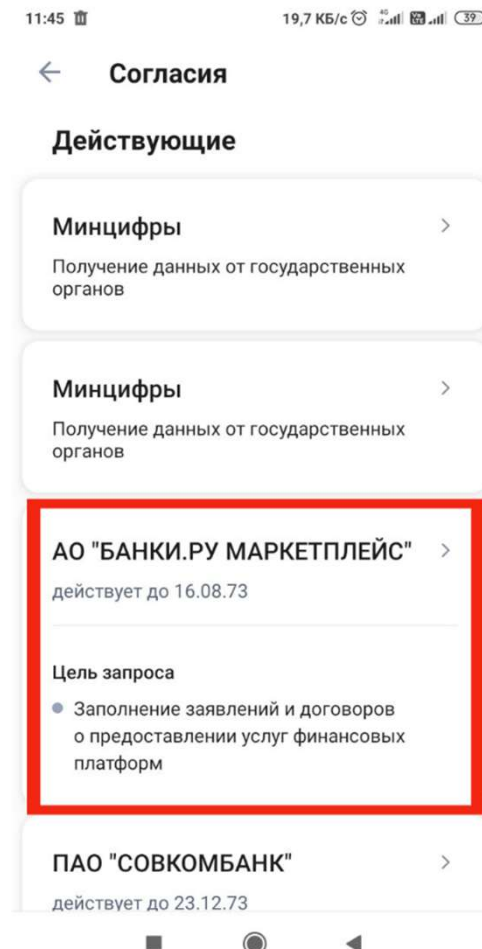
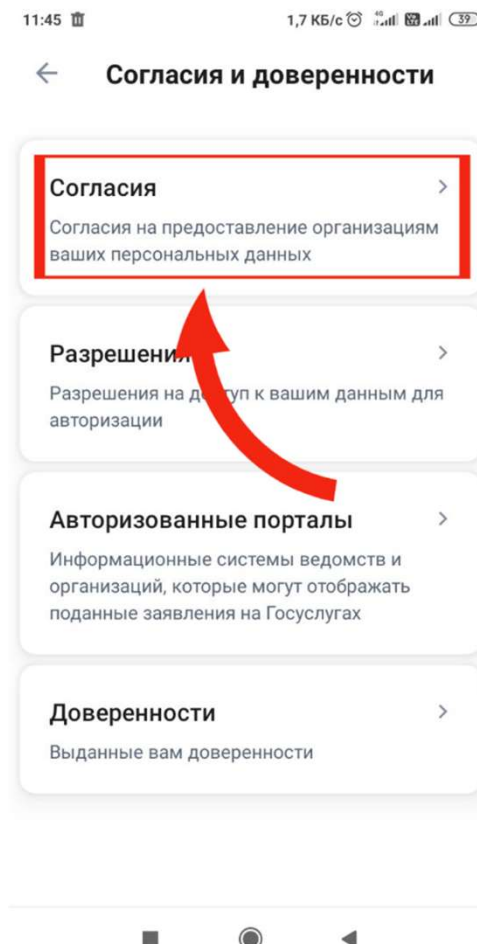
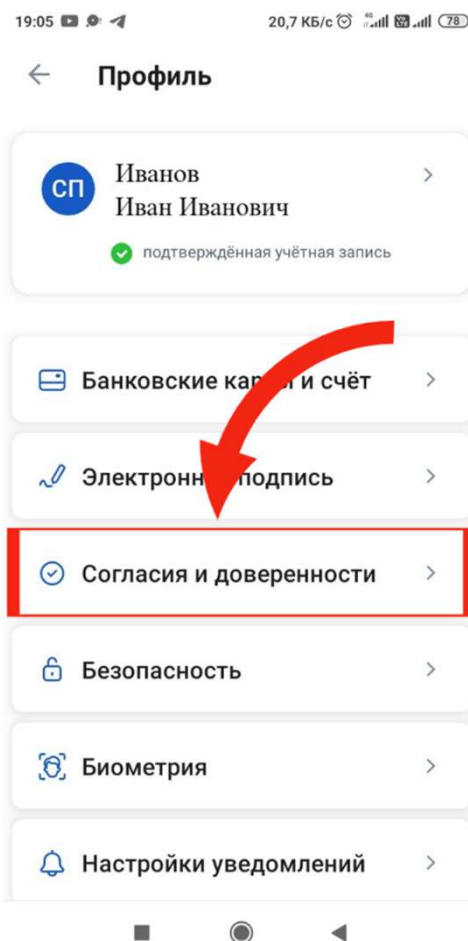
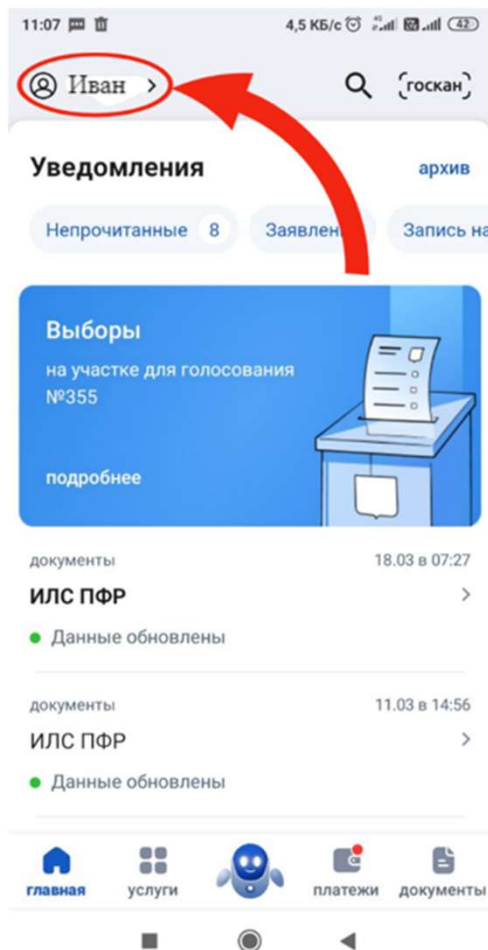
Функция восстановления доступа контрольным вопросом.

После переоформления SIM-карты, мошенники не смогут восстановить доступ к личному кабинету, так как они не знают ответ на контрольный вопрос.





Отзыв согласий





Отзыв согласий

11:45 0,1 КБ/с

← **Согласие**

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Запрашиваемые персональные данные

- Дата рождения, указанная в документе, удостоверяющем личность
- Сведения о водительском удостоверении (страна выдачи, серия, номер, дата выдачи и прекращения действия, орган, выдавший водительское удостоверение, разрешенные категории вождения)
- Сведения о паспорте, удостоверяющем личность гражданина Российской Федерации (серия, номер, дата выдачи и прекращения действия, орган, выдавший паспорт)

Отозвать согласие

личности: серия и номер документа, дата

11:45 0,0 КБ/с

← **Согласие**

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Отзыв согласия

АО "БАНКИ.РУ МАРКЕТПЛЕЙС" больше не будет получать ваши данные из личного кабинета на Госуслугах

Организация вправе продолжить обработку уже полученных данных

- Если этого требуют условия действующего договора между вами и организацией
- По основаниям ч. 1 ст. 6 Закона о персональных данных

Отменить **Отозвать**

11:46 20,2 КБ/с

← **Согласия**

Действующие [архив](#)

Минцифры >

Получение данных от государственных органов

Минцифры >

Получение данных от государственных органов

ООО "ХКФ БАНК" >

действует до 11.03.74

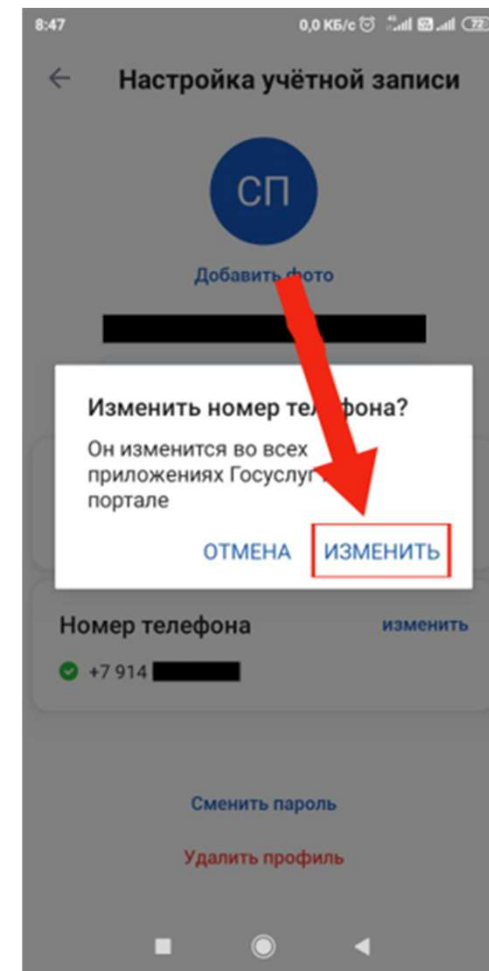
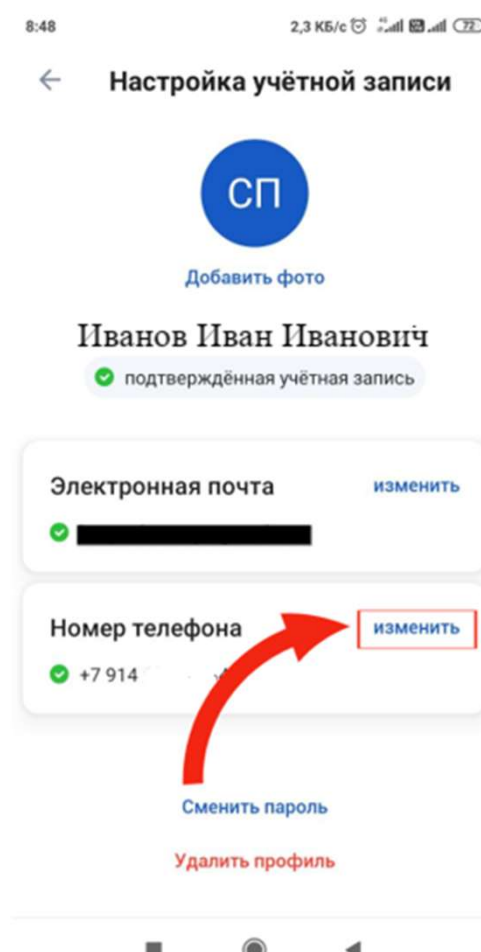
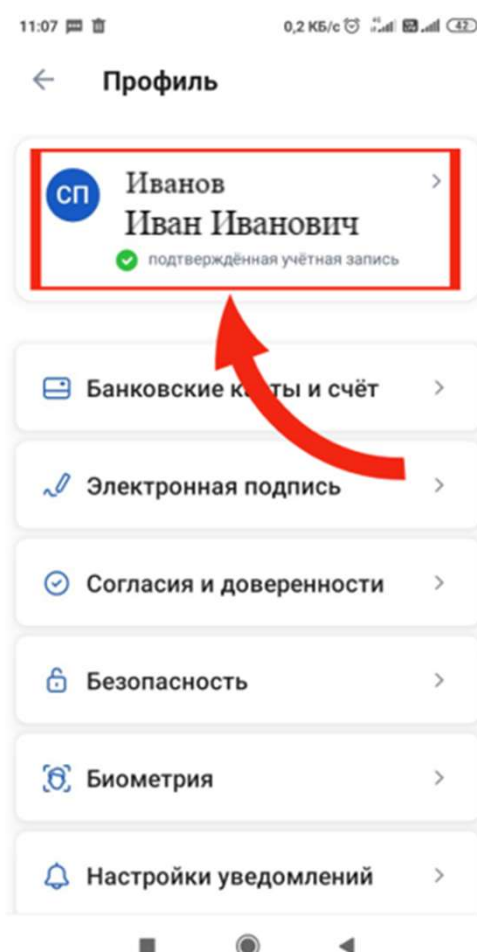
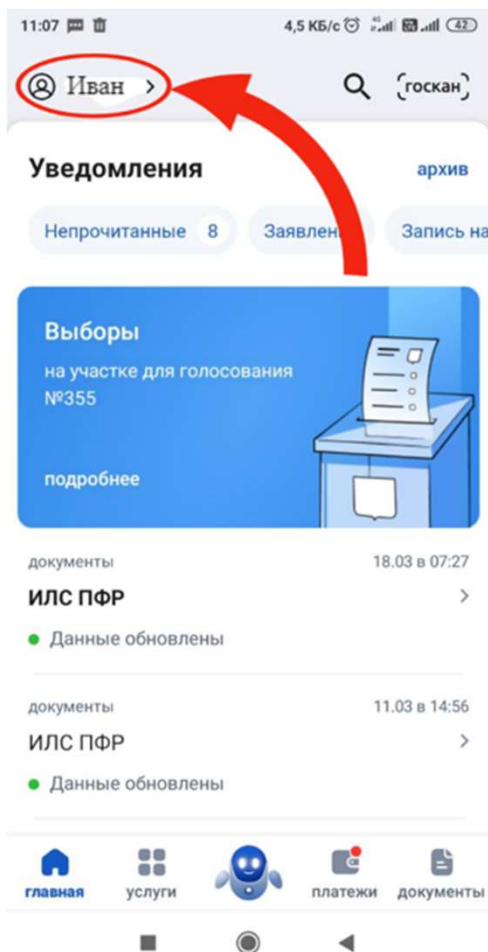
Цель запроса

- Предоставление кредита (займа), в том числе кредита с лимитом кредитования и (или) овердрафта, выдача и обслуживание банковской карты для обслуживания кредита (займа)

Согласие отозвано ✕



Способ открепления номера телефона

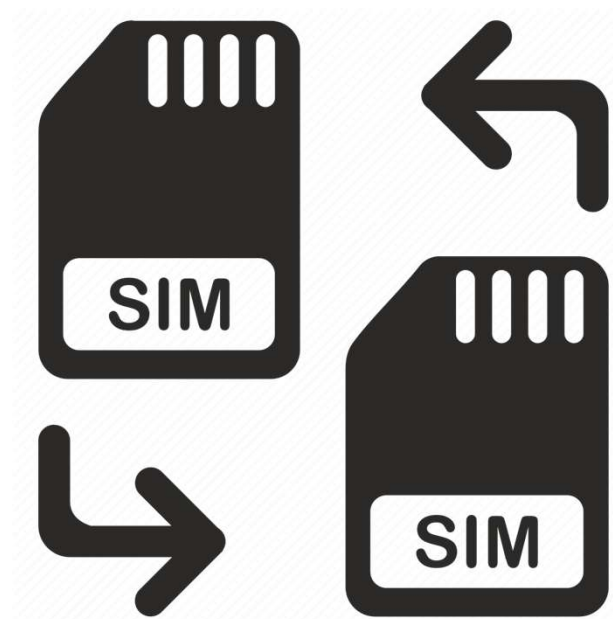




2. Переоформление SIM-карты

SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

Тем самым, предоставляя возможность новому пользователю восстановить доступ к личному кабинету от портала «Госуслуги», путем ввода SMS-кодов, поступивших на перевыпущенный номер SIM-карты, что и делают злоумышленники.





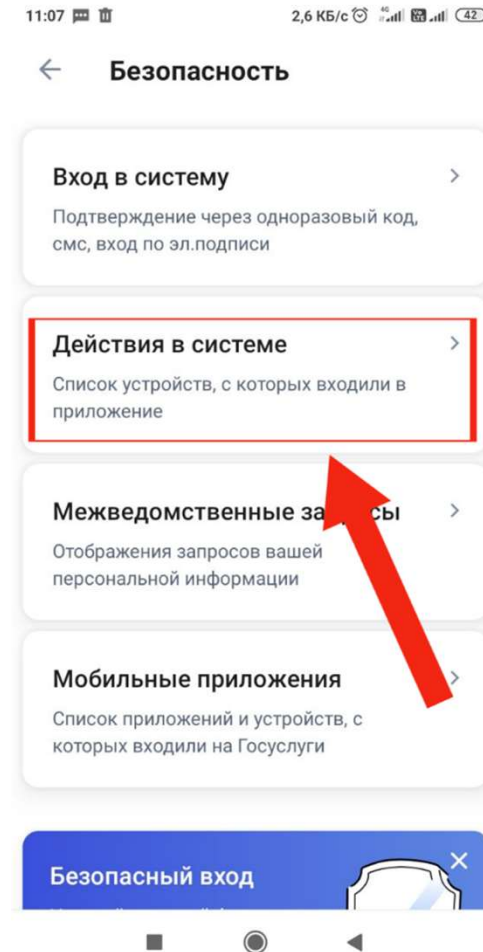
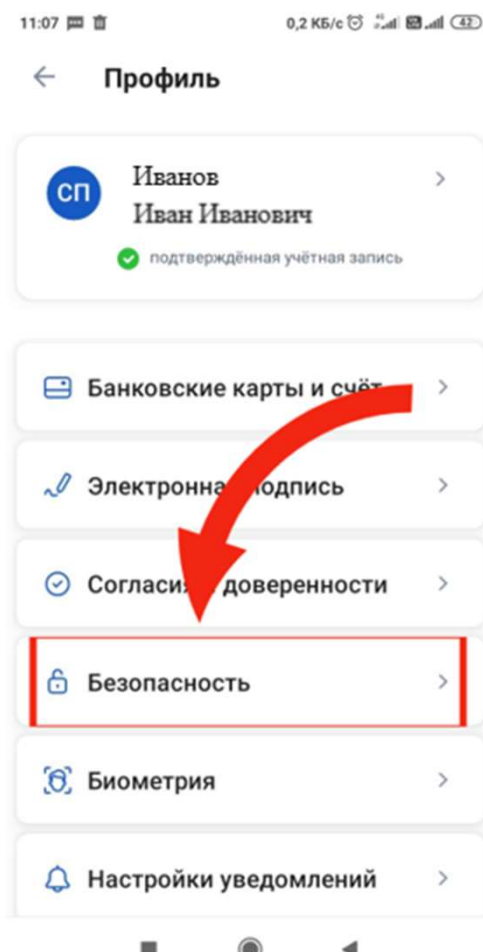
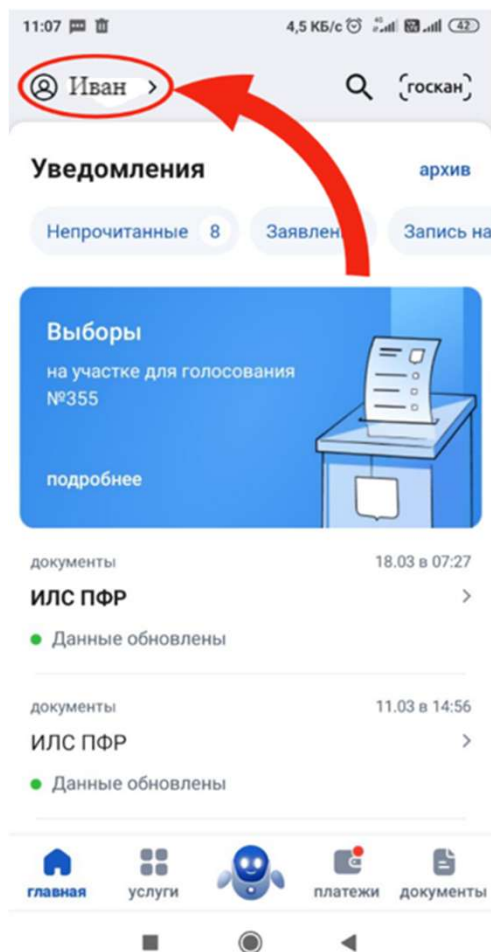
Мошенники взломали личный кабинет портала «Госуслуги»



МУ МВД России «Иркутское»



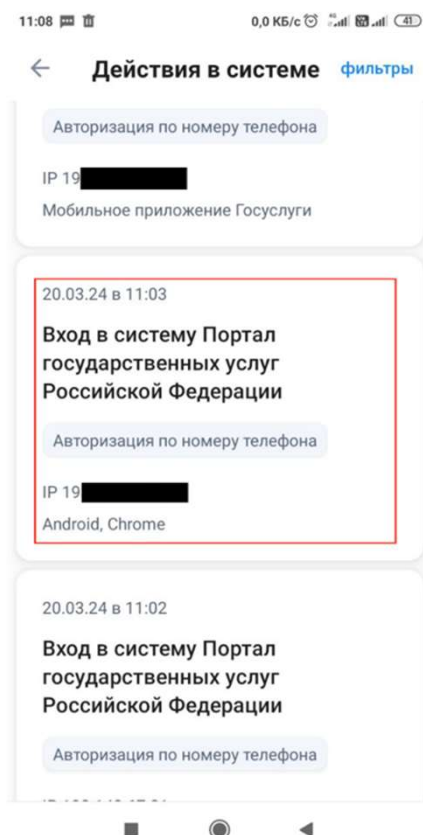
Признаки взлома личного кабинета портала «Госуслуги»





Признаки взлома личного кабинета портала «Госуслуги»

Без признаков взлома



С признаками взлома

2023-09-01T19:06:17.120+0300	Вход в систему Vivus.SMSFinance. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:54:47.939+0300	Вход в систему Портал государственных услуг Российской Федерации. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:51:03.165+0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:45:07.170+0300	Вход в систему ООО МФК "ВЭББАНКИР" . Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:44:10.675+0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49

Восстановите пароль от личного кабинета

Перейдите на сайт или в приложение одного из своих банков.

Повторите регистрацию на «Госуслуги» через банк-номер из личного кабинета банка будет перенесен в личный. Банк вышлет пароль для входа в аккаунт.

ИЛИ



Обратитесь в офис МФЦ и попросите оператора восстановить пароль.

Сотрудники проверят вашу личность, помогут восстановить доступ к аккаунту и сменить пароль.

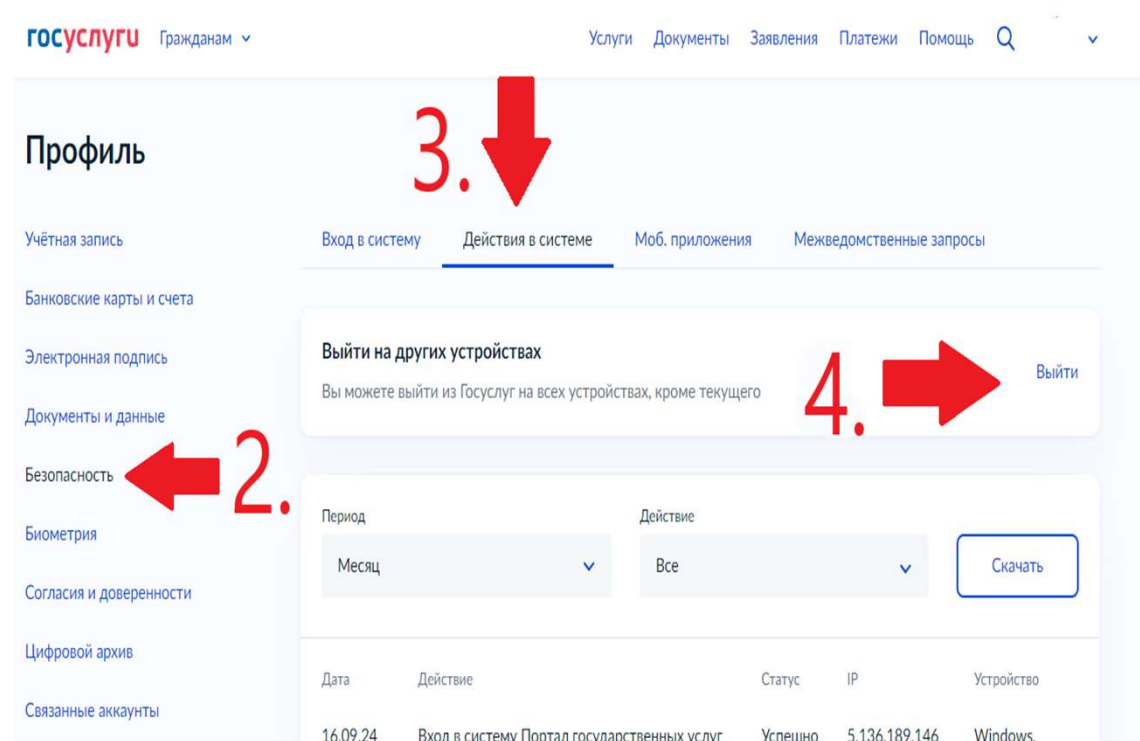
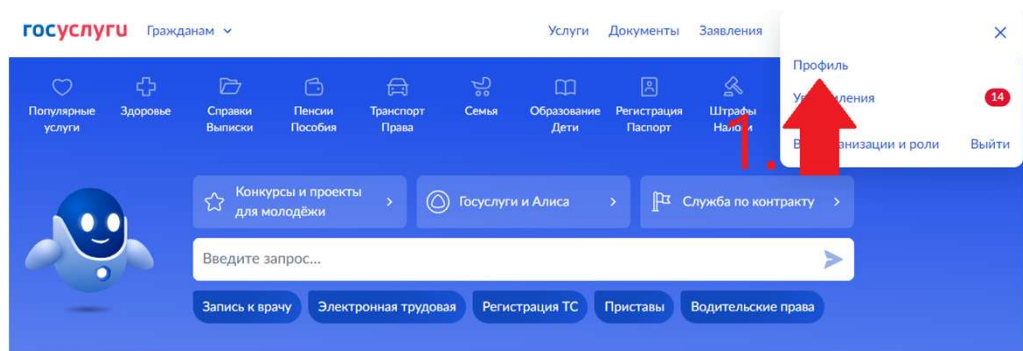
Возьмите с собой паспорт и СНИЛС



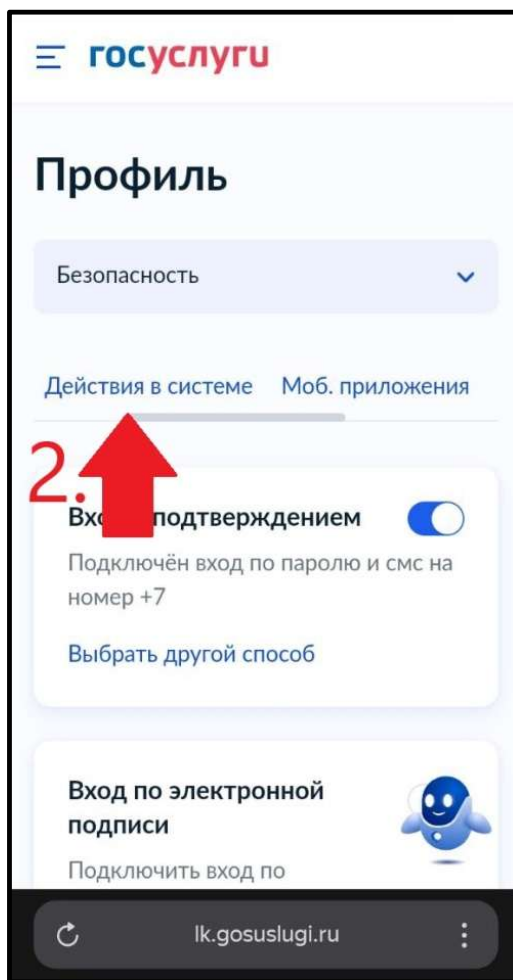
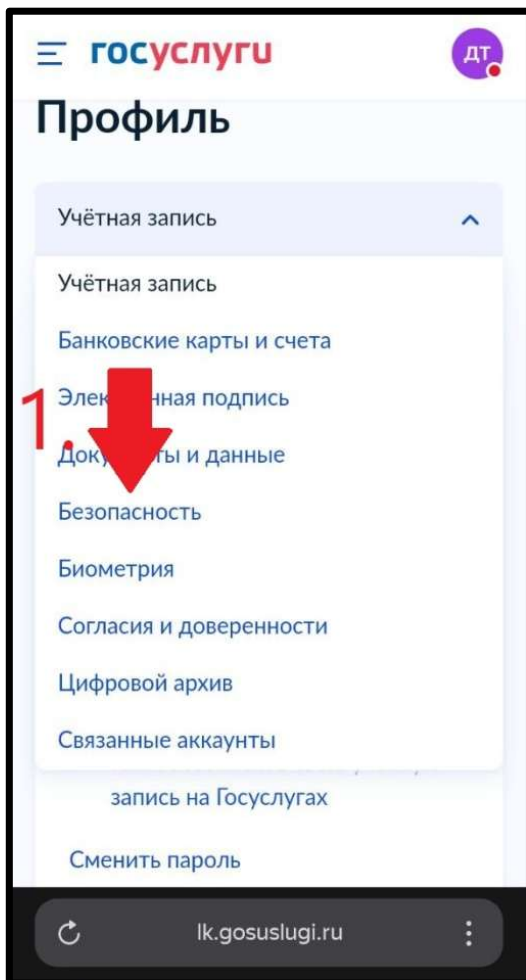
Определите, где использовалась учетная запись

Вы можете выйти одновременно на всех устройствах, кроме текущего

НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ:



НА МОБИЛЬНОМ ТЕЛЕФОНЕ



Отзовите разрешения, которые не выдавали.

Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени.



Обратитесь в полицию и подайте заявление.



При наличии данных, указывающих на совершение противоправных действий, в том числе связанных с мошенничеством, подайте заявление в полицию.

Возьмите с собой копию заявления из МФЦ, скриншоты СМС – сообщений и другие доказательства.



Проверьте кредитную историю и узнайте, направлялись ли от вашего имени заявки на займы

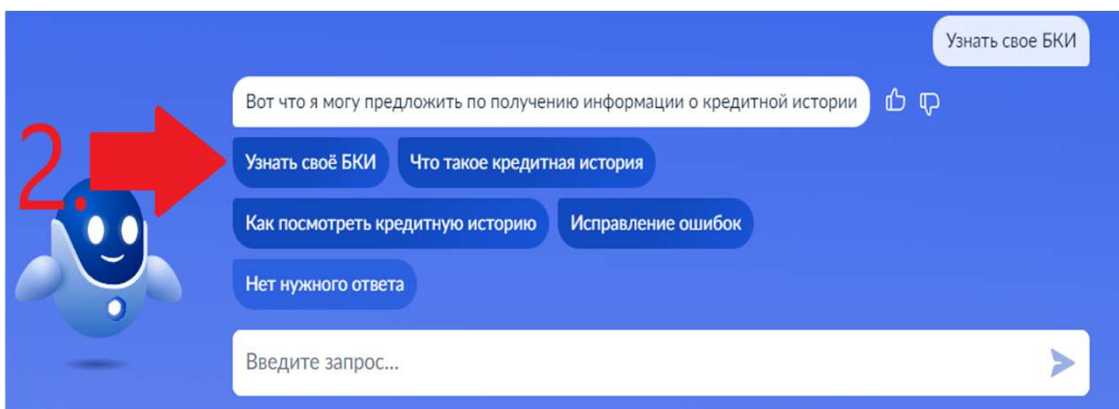
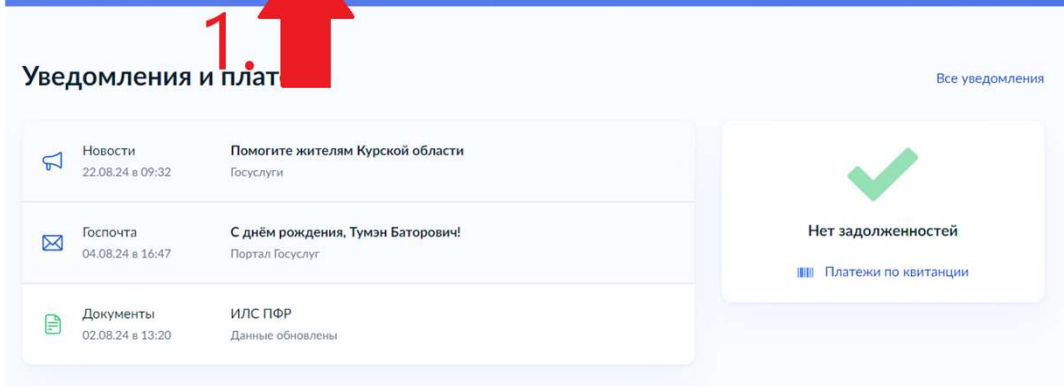
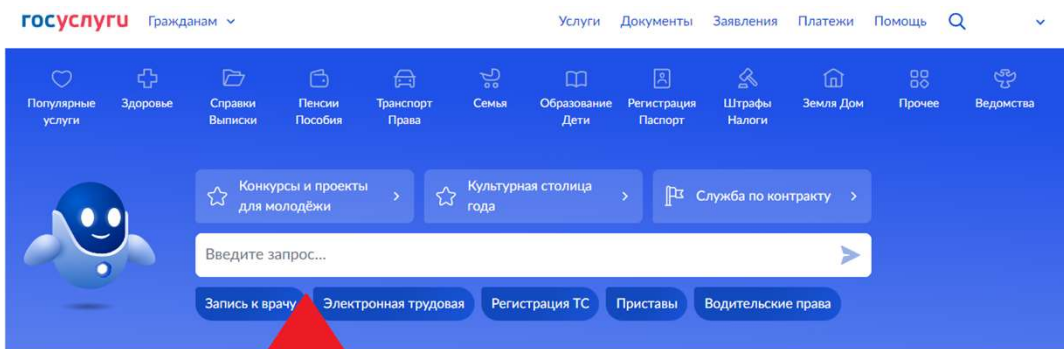


Выясните, в каких бюро хранится ваша кредитная история (их может быть несколько).

Сделать это можно на портале «Госуслуги»:

- 1. Введите в строке поиска запрос «узнать свое БКИ».**
- 2. Далее зарегистрируйтесь на сайте каждого бюро* и запросите свою кредитную историю (рекомендуем направить запрос через 2 недели после взлома аккаунта).**

***Можно авторизоваться с помощью учетной записи «Госуслуги».**



Узнать на портале «Госуслуги» в каких бюро хранится ваша кредитная история.

